REMARKS

I. Introduction

In response to the Office Action dated January 22, 2007, new claim 1 as been added. Claims 1, 2, 4-29, and 31-51 are in the application. Re-examination and re-consideration of the application, as amended, is requested.

II. Examiner Interview

Reference is made to a telephonic conversation between Examiner Tran and Attorney Georgann Grunebach and a subsequent telephonic conversation between Examiner Tran, Attorney Georgann Grunebach and Attorney Victor Cooper, in which the notion of amending the claims to accept allowable subject matter was discussed. The Applicant elected against the proposed amendment.

III. Allowable Subject Matter

The Office Action indicates that the subject matter of claims 2 and 29 would be allowable if written in independent form including all of the limitations of the base claim and any intervening claims] The Applicants acknowledge the Office Action's indication of allowable subject matter, but traverse the rejection of the remaining claims. Should the rejection of these claims be maintained, the Applicants will make suitable amendments to present the allowable claims in independent form.

IV. The Cited References and the Subject Invention

A. The Okabe Reference

U.S. Patent No. 6,889,208, issued May 3, 2005 to Okabe et al. disclose a contents sale system. In a contents sale system, original contents data are encrypted into encryption-resultant contents data in response to original playback key data. The original playback key data are encrypted into first encryption-resultant playback key data. The first encryption-resultant playback key data are encrypted into second encryption-resultant playback key data in response to an ID of a sale destination terminal apparatus. The encryption-resultant contents data and the second encryption-resultant playback key data are transmitted to the sale destination terminal apparatus. The sale

destination terminal apparatus is enabled to decrypt the second encryption-resultant playback key data into the first encryption-resultant playback key data in response to the ID of the sale destination terminal apparatus. The sale destination terminal apparatus is enabled to decrypt the first encryption-resultant playback key data into the original playback key data. The sale destination terminal apparatus is enabled to decrypt the encryption-resultant contents data into the original contents data in response to the original playback key data.

B. The Akins Reference

U.S. Patent No. 6,560,340, issued May 6, 2003 to Akins et al. disclose a method and apparatus for geographically limiting service in a conditional access system. A cable television system provides conditional access to services. The cable television system includes a headend from which service "instances", or programs, are broadcast and a plurality of set top units for receiving the instances and selectively decrypting the instances for display to system subscribers. The service instances are encrypted using public and/or private keys provided by service providers or central authorization agents. Keys used by the set tops for selective decryption may also be public or private in nature, and such keys may be reassigned at different times to provide a cable television system in which piracy concerns are minimized.

V. Office Action Prior Art Rejections

In paragraphs (6)-(7), the Office Action rejected claims 1, 28, and 43 under 35 U.S.C. § 103(a) as unpatentable over Okabe et al., U.S. Patent No. 6,889,208 (Okabe). The Applicants respectfully traverse these rejections.

With Respect to Claim 1: Claim 1 recites:

A method of storing program material in a media storage device communicatively coupled to a receiver for subsequent replay, comprising the steps of:

(a) accepting encrypted access control information and the program material encrypted according to a first encryption key in the receiver, the access control information including a first encryption key and control data;

(b) decrypting the received access control information in a conditional access module releasably coupleable with the receiver to produce the first encryption key;

(c) decrypting the program material using the first encryption key;

(d) re-encrypting the program material according to a second encryption key;

(e) encrypting the second encryption key in the conditional access module according to a third encryption key to produce a fourth encryption key; and

(f) providing the re-encrypted program material and the fourth encryption key for storage.

The Applicants respectfully disagree that the Okabe reference discloses the features of claim 1. Claim 1 recites the step of

(a) accepting encrypted access control information and the program material encrypted according to a first encryption key in the receiver, the access control information including a first encryption key and control data;

The First Office Action appeared to analogize to the first player terminal apparatus receiving the primary encryption resultant playback key data and the encryption resultant contents data:

> A customer's player 6*a* can be connected to the terminal apparatus 5 via an IEEE1394 interface. The player 6*a* includes a computer which operates in accordance with a control program stored in a memory. The control program is designed to enable the player 6*a* to implement processes mentioned later. The player 6*a* also includes a storage unit. A predetermined ID (a predetermined identification code word) is assigned to the player 6*a*. In the case where the player 6*a* is connected with the terminal apparatus 5, the player 6*a* informs the terminal apparatus 5 of its own ID before downloading. The terminal apparatus 5 separates the composite data into the primary encryption-resultant playback key data and the encryption-resultant contents data.

The Second Office Action indicated:

> "The Examiner notes, the Okabe reference teaches 'The terminal apparatus 5 separates the composite data into the primary encryption-resultant playback key data and the encryption-resultant contents data'. The control information, the control information is interpreted to have the same meaning as 'the encryption resultant contents data' in the Okabe reference. Note the Okabe reference uses the terms 'encryption-resultant playback key' and 'encryption resultant content data'. The control information is contained in the header of the encryption resultant content data header, see Okabe col. 8, lines 27-45.

The Examiner analogizes the Applicant's "control information" with the "control information" recited in claim 1. However, there are structural differences between Okabe's "control information" and the Applicants' "control information."

Claim 1 recites "encrypted access control information ...[that includes] a first encryption key and control data." In other words, the first encryption key and the control data together make up the "control information" and that "control information" is encrypted.

Osaka's "control information" is not packaged with the key at all. Plainly, it is instead packaged with the media program:

> Music-related data transferred from the terminal apparatus **5** to the player **6***a*, and music-related data transferred from the player **6***a* to the player **6***b* are of a given format. Specifically, the music-related data transferred from the terminal apparatus **5** to the player **6***a* contain a sale header, a sale sub header, and encryption-resultant contents data. Similarly, the music-related data transferred from the player **6***a* to the player **6***b* contain a sale header, a sale sub header, and encryption-resultant contents data. The encryption-resultant contents data include a contents header, a sound stream, text data, and extension data. The sound stream represents music contents. The text data represent tune names and artist names.
>
> As shown in FIG. 2, the sale header has a size of 64N+M bytes which depends on the number "N" of tunes in the sale contents, where "M" denotes a predetermined natural number. In the sale header, one byte (the 4-th byte) is occupied by transfer control data, and K bytes, that is, the (64N+M-K)-th byte to the (64N+M)-th byte, are occupied by encryption-resultant playback key data (secondary encryption-resultant playback key data). Here, "K" denotes a predetermined natural number.
>
> Specifically, bytes of the sale header in FIG. 2 are sequentially assigned to indications of different items as follows.
>
> 1 byte of a sale header version;
> 1 byte of a sale header size;
> 1 byte reserved;
> 1 byte of transfer control data;
> 8 bytes of a contents sale ID;
> 8 bytes of a transmission source ID;
> 2 bytes of a sale ticket number;
> 1 byte of a sale sub header number;
> 1 byte of a contents tune number;
> 32 bytes of a manufactured article title;
> 16 bytes of a manufacturer's name;
> 4 by N bytes of data lengths of respective tunes;
> 8 by N bytes of the names of the respective tunes;
> 8 by N bytes of the names of artists of the respective tunes;
> 4 by N bytes of the play times of the respective tunes; and
> K bytes of encryption-resultant playback key data.

Therefore, Okabe fails to disclose step (a) of the Applicants' invention.

Claim 1 then recites the step of

(b) decrypting the received access control information in a conditional access module releasably coupleable with the receiver to produce the first encryption key

Which the Office Action indicates is disclosed by the first player (6b) decrypting recovering the original contents data:

> storage unit of the player 6*a*. The player 6*a* recovers original contents data by decrypting the encryption-resultant contents data. In addition, the player 6*a* generates other secondary encryption-resultant playback key data (third encryption-resultant playback key data) which will be used for data transfer or data copying to another player.

This is incorrect. The foregoing only discloses that the player recovers the original contents data by decrypting it. It does not disclose the step of decrypting the received access control information in a conditional access module to produce the first encryption key.

The Second Office Action disagrees., stating:

> The Examiner disagrees this is clearly shown in Okabe see col. 7, lines 13-38, which teach how material is received by a player. The material received is the content as well as the control data, which is interpreted to be the 'encryption resultant data' in Okabe. The module is further able to copy the data according to the decrypted resultant data, i.e. control data.

As pointed out above, claim 1 recites that the access control information is packaged with the encryption key, not with the encrypted media program (as in Okabe). This difference confused the Applicants as to how Okabe could possibly teach decrypting the "control information" (the recited portion of the Okabe reference (col. 7, lines 13-38 clearly does not do so).

The Second Office Action clarifies the Examiner's position. It analogizes the Applicants' decryption of the control information, to Okabe's decryption of the media program (which includes the control information). This indeed does appear to be disclosed by Okabe.

Claim 1 then recites the step of

(c) decrypting the program material using the first encryption key;

The First Office Action indicates that this is disclosed as follows;

> storage unit of the player 6*a*. The player 6*a* recovers original contents data by decrypting the encryption-resultant contents data. In addition, the player 6*a* generates other sec- 35

The foregoing indicates that the original contents data is recovered by decryption, but it does not indicate which key is used to accomplish this feat.

The Second Office Action disagrees:

"The Examiner disagrees with this argument and notes that Okabe clearly shows that the data distributed to the player is the encryption key as well as the encryption resultant content data. The encryption resultant playback key is used to decrypt the data."

The Applicants' respond that the above-quoted passage of Okabe plainly does not indicate which key is sued to decrypt the data. The Applicants do concede however, that as they understand the Okabe reference, the decryption of the encryption-resultant data is likely performed using the encryption-resultant playback key.

Claim 1 next recites:

> *(d) re-encrypting the program material according to a second encryption key*

Analogizing this step to operations performed in player 6a, the First Office Action indicates that this is disclosed in Okabe as follows:

> storage unit of the player 6*a*. The player 6*a* recovers original contents data by decrypting the encryption-resultant contents data. In addition, the player 6*a* generates other sec- 35
> ondary encryption-resultant playback key data (third encryption-resultant playback key data) which will be used for data transfer or data copying to another player.

This is incorrect. At no point does player 6a *re-encrypt* program material at all, nor does it do so with a *second key* different than the key by which it was encrypted when it was received by the player 6a (which the Office Action analogizes to Claim 1's "first key"). Instead, Okabe encrypts generates "other secondary encryption-resultant playback key data",

> tents data. In addition, the player 6*a* generates other sec- 35
> ondary encryption-resultant playback key data (third encryption-resultant playback key data) which will be used for data transfer or data copying to another player.

and then sends that data, along with the same "encryption resultant contents data" that was received from the terminal apparatus 5 to the second player 6b.

> player 6*b*. In the case where the player 6*b* is connected with the player 6*a*, the player 6*b* informs the player 6*a* of its own ID before contents data are transferred or copied. During the data transfer, the copy-source player 6*a* transmits the encryption-resultant contents data and the secondary encryption-resultant playback key data into the storage unit of the copy-destination player (the transfer-destination player) 6*b*. Thus, the encryption-resultant contents data and the secondary encryption-resultant playback key data are copied.

Okabe therefore does not disclose step (d) of claim 1.

The Second Office Action disagrees:

The Examiner disagrees with this argument and notes, that a second encryption resultant content data are generated, this is the same meaning as re-encrypting.

However, ***this is incorrect***. The clause in question is:

(d) re-encrypting the program material according to a second encryption key

The foregoing recites that the program material is re-encrypted using a second key. The Second Office Action indicates at "a second encryption resultant content data are generated," but this is not true. The Applicant has carefully searched the Okabe reference and can find no such disclosure. Okabe does describe generating a second encryption resultant playback key, but it does not describe the generation of "second encryption resultant content data." If Okabe indeed discloses this feature, the Applicants ask that the Examiner indicate, by column and line, where Okabe does so.

Steps (e) and (f) of claim 1 recite:

(e) encrypting the second encryption key in the conditional access module according to a third encryption key to produce a fourth encryption key; and

(f) providing the re-encrypted program material and the fourth encryption key.

The First Office Action acknowledges that steps (e) and (f) are not disclosed in Okabe. This is plainly so, but not only for the reasons the Office Action suggests. Step (e) of claim 1 recites that

the *second key*, which was used *to re-encrypt the program material* (a step that is not disclosed in Okabe) is then encrypted in the conditional access module according to a third encryption key to produce a fourth encryption key; and step (f) recites that this re-encrypted program material (and the fourth encryption key) is provided for storage external to the conditional access module. Since Okabe does not disclose re-encrypting the program material with a second key at all (it does not disclose step (d)), none of these steps can possibly be disclosed either.

The Second Office Action disagrees:

> The Examiner disagrees with [this argument] and notes that the player generates other second encryption resultant playback key data, the generating of this second or third resultant playback key data has the same meaning

Again, this is incorrect. Clause (d) of claim 1 recites the re-encryption of the program material, NOT the key.

Nonetheless, the First Office Action argues:

(1) That it would be obvious to modify Okabe to control the number of copies generated, and

(2) That it would be obvious to do so by generating a new encryption key.

The Applicants disagree with both assertions.

Okabe does not have to be modified to control the number of copies generated. Okabe controls the number of copies generated, without modification and this is accomplished via a transfer generation number, which is part of the sale header, which is part of the music-related data transferred from the terminal apparatus to the player 6a to the second player 6b.

Since Okabe already controls the number of copies generated, there is no reason to modify it to do so.

The First Office Action asserts that Okabe discloses that "each time the transfer generation number, and the encryption resultant playback key data are updated, another key is generated", but the Applicants can find no part of Okabe that discloses this feature.

The Second Office Action states:

> "... Okabe discloses generating 'encrypted resultant content' each time the material is distributed. The number of the key used for encryption/decryption is obviously incremented each time the resultant playback key is generated, i.e. second or third."

The Applicants have searched Okabe and find nothing in it to suggest generating "encrypted resultant content" each time material is distributed. If Okabe indeed discloses this feature, the Applicants respectfully request that the Examiner indicate where such disclosure might be found. What Okabe does disclose is a new encryption-resultant playback key, but of course, that is an entirely different thing.

Further, Okabe discloses a system where new encryption resultant playback keys are generated (using the ID of the destination player) each time a copy is generated for a new player. Accordingly, the Applicant does not understand why the Second Office Action asserts that the key is "incremented".

The bottom line is that Okabe does not perform step (d) of the Applicant's invention (re-encrypting the program material according to a second encryption key), and there is no teaching to modify it to do so. Since it does not teach this feature, steps (e) and (f) (which use the re-encrypted program material) are likewise not disclosed or taught.

Okabe, in fact, teaches away from such a modification, because the "encryption resultant contents data" remains is never "re-encrypted" ... not by the terminal, not by the first player, nor by the second player. If it were to be decrypted and re-encrypted with a key, that key would have to be disseminated to each of the subsequent players, and Okabe surely does not provide a motivation for doing so or suggest how this might be done.

Finally, claim 1 has been amended to recite that the re-encrypted program material and the fourth key is provided for storage external to the conditional access module. The First and Second Office Actions have alleged that the step (b) "decrypting the received access control information in a conditional access module releasably coupleable with the receiver" is analogous to operations taking place in Okabe's "player," Okabe can meet the external storage feature only if it discloses storing the encrypted program external to the conditional access module, and plainly, it does not.

Claim 28 recites analogous features and is patentable for the same reasons.

Claim 43 is dependent upon claim 28 and is patentable for the same reasons as well.

In paragraph (8), claim 4-16, 31-42, and 44-46 were rejected under 35 U.S.C. § 103(a) as unpatentable over Okabe in view of Akins. In paragraph 9, claims 17-27 and 47-50 as rejected as unpatentable over Okabe in view of Akins. The Applicant respectfully traverses these rejections.

With Respect to Claim 15 and 41: Claim 15 recites:

The method of claim 1, wherein the control data is temporally-variant.

The First Office Action indicated these steps are disclosed in Okabe. This rejection has been withdrawn and instead, these claims are rejected as disclosed in Okabe in view of Akins. The Second Office Action remarks:

> " ... Akins clearly shows that the content data can contain time limitations as to how long the distributed content can be viewed in col. 28, line 43 through col. 29 line 39."

The appropriate portion of Akins is reproduced below:

Update Entitlement Agent Properties

This EMM contains the values for EA fields **1516** of EAD **1409**. EA administration EMM code **1317** reads EMM header **1113** to get the EAID for the EA to which the EMM is directed and simply sets fields **1516** in EAD **1409** for the EA from the EMM.

Non-Event Broadcast EMMs

Of the non-event broadcast EMMs, four types will be discussed here. These are Update MSK, Update Bit Map, Update List, and update combinations with MSK and list or bitmap. Those skilled in the art will be able to easily apply the principles explained below to EMMs that perform the functions indicated by the names of the other non-event broadcast EMMs. For example, the principles of digital EMMs can be applied to analog EMMs. There is a separate type of NVSC **1405** for each information type provided by the above non-event broadcast EMMs. FIG. **16** shows the contents of four of these types of NVSCs. Each NVSC type will be discussed together with the EMM that provides the information it contains.

Update MSK

The Update MSK EMM is used to send a new MSK for a set of services provided by the EA specified by the EMM. The new MSK and other information associated with the MSK are stored in MSK NVSC **1601** in list **1411** for EA information **1333** belonging to the EA specified by the EMM. Included in MSK NVSC **1601** is header **1502**. Header **1502** specifies that NVSC **1601** is a MSK NVSC, gives the NVSC's name, and contains next element pointer **1507** to the next element in list **1411**. The other fields contain information about the MSK. In the preferred embodiment, MSK **1608** has two 128-bit parts: the even MSK **1609** and the odd MSK **1611**. Each part has two halves, i.e., a first half and second half, each of which has 56 key bits and 8 unused parity bits. The MSK **1608** is associated with a pair identifier **1603** for MSK **1608**, an expiration date **1605** for MSK **1608**, and a flag **1607** indicating whether the value of expiration date **1605** should be ignored. If the expiration date **1605** is not to be ignored, DHCTSE **627** will not use MSK **1608** to decrypt a control word after the expiration date. The identifier **1603** is per-EA, and consequently, a given EA may have one or more MSK NVSCs **1601** at any given time to store a plurality of different MSKs. Thus, conditional access system **601** not only permits separate security partitions for each EA, but also permits security partitions within an EA.

The Update MSK EMM header contains the EAID needed to locate EA information **1333** for the EA; the message contains the name of the NVSC that is to receive the MSK, a MSK pair selector which specifies a MSK pair ID for the MSK to be updated, a set of flags permitting the EA to selectively change MSK pair ID **1603**, expiration date **1605**, no expiration date **1607** and either half of MSK **1608**, and the information needed to make the changes. At a maximum, the EMM contains a value for MSK pair ID **1603**, a value for expiration date **1605**, a value for no expiration date **1607**, and values for even MSK **1609** and odd MSK **1611**. EA MSK code **1319** processes the Update MSK EMM by locating EA Information **1333** for the EA identified by the EMM header's EAID, using the cell name to locate the proper NVSC, giving that NVSC the MSK type, and then writing to the MSK NVSC **1601** as required by the flags and the information in the EMM. This procedure is the same for both analog and digital Update MSK EMMs. The differences are in the EMM command code in EMM Header **1123** and NVSC type **1503**.

The foregoing discloses that keys may have an expiration time. Associating an expiration with a key is not analogous to *temporally variant* access control information. For example, a key that changes over time is not analogous to a key that has an expiration time.

Claims 41 recite analogous features and are patentable for the same reasons.

With Respect to Claim 17: Claim 17 recites:

An apparatus for storing program material encrypted according to a first encryption key for replay, comprising:

a conditional access module, for accepting encrypted access control information including the first encryption key and temporally-variant control data, the control access module comprising:

a first decryption module, for decrypting the access control information to produce the first encryption key;

a first encryption module, for encrypting a second encryption key with a third encryption key to produce a fourth encryption key; and

a second decryption module for decrypting the fourth encryption key to produce the second encryption key.

Claim 17 recites that the control data is temporally variant. This claim was originally rejected as unpatentable over Okabe. It is not rejected as unpatentable over Okabe in view of Akins. However, as described above, neither Akins does teach this feature either.

In their first response, the Applicants pointed out that Okabe does not disclose anything equivalent to a second encryption key (because it does not decrypt the media program and re-encrypt it ... the second player passes the encrypted program material to the second player in the same form as it is received). Also, they pointed out that Okabe does not disclose anything like a second decryption module for decrypting the fourth encryption key to produce the second encryption key. That feature is not only undisclosed, Okabe plainly teaches against it. The whole point of Okabe is to transfer a program from the first player to the second ... it does not even remotely suggest transferring the same program from the second player back to the first as must be the case if the Office Action's analogies are adopted. Indeed, there would be no reason whatsoever to do so. That being the case, the Applicant's questioned what motivation could there be for modifying Okabe to add a second decryption module for decrypting the fourth encryption key to produce the second encryption key?

The Second Office Action answers:

> The Examiner disagrees, and notes that Okabe discloses that the player produces secondary encrypted resultant content, the encrypted resultant content, is the program re-encrypted.

The Applicants respond that they have looked in Okabe and can find no reference to secondary encrypted resultant content ... only secondary encrypted playback keys.

With Respect to Claims 18: Claim 18 recites:

The apparatus of claim 17, further comprising:

a tuner, communicatively coupleable to the conditional access module for receiving the encrypted access control information and the program material encrypted according to a first encryption key;

a third decryption module, for decrypting the program material using the first encryption key produced by the conditional access module;

a second encryption module, for re-encrypting the decrypted program material according to the second encryption key; and

a fourth decryption module, for decrypting the re-encrypted program material according to the second encryption key.

As described above, Okabe does not disclose a second encryption module for re-encrypting the decrypted program material according to a second encryption key ... the encrypted media program is passed from the terminal to the first player to the second player without decryption and re-encryption. Also lacking is the fourth decryption module.

The Second Office Action replies that the program material is re-encrypted with subsequent keys, but as described above, Okabe does not re-encrypt the program materials ... only the playback keys.

The Second Office also suggests that the Claim 18's "fourth key" is interpreted to be equivalent to the second or third keys. The Applicants are not sure which "second or third keys" the Examiner is referring to, and the Applicants indicated that Okabe did not disclose a fourth decryption module, not a fourth key.

With Respect to Claim 25: Claim 25 recites that the second encryption key is stored in the conditional access module. The First Office Action suggests that this is disclosed as follows:

> A customer's player 6*a* can be connected to the terminal apparatus 5 via an IEEE1394 interface. The player 6*a* includes a computer which operates in accordance with a control program stored in a memory. The control program is designed to enable the player 6*a* to implement processes mentioned later. The player 6*a* also includes a storage unit. A predetermined ID (a predetermined identification code word) is assigned to the player 6*a*. In the case where the player 6*a* is connected with the terminal apparatus 5, the player 6*a* informs the terminal apparatus 5 of its own ID before downloading. The terminal apparatus 5 separates the composite data into the primary encryption-resultant playback key data and the encryption-resultant contents data. The terminal apparatus 5 encrypts the primary encryption-resultant playback key data into secondary encryption-resultant playback key data (second encryption-resultant playback key data). In the case where the terminal apparatus 5 is connected with the player 6*a*, the terminal apparatus 5 downloads the encryption-resultant contents data and the secondary encryption-resultant playback key data into the storage unit of the player 6*a*. The player 6*a* recovers original contents data by decrypting the encryption-resultant contents data. In addition, the player 6*a* generates other secondary encryption-resultant playback key data (third encryption-resultant playback key data) which will be used for data transfer or data copying to another player.

but nothing in the foregoing discloses the use of a second encryption key for re-encrypting the decrypted program.

The Second Office Action replies that Okabe teaches that a second key is generated with the second encryption resultant content. However, as described above, Okabe does not disclose generating second encryption resultant content ... only a second encryption resultant playback key.

In paragraph 11, the Office Action rejected claims 4-14, 16, 19-24, 31-35, 37-39, 42 and 44-50 under 35 U.S.C. § 103(a) as unpatenable over Okabe and Akins.

Applicants respectfully traverse these rejections.

With Respect to Claim 4: Claim 4 recites:

The method of claim 1, wherein the conditional access module is implemented on a smartcard.

Claim 1 recites that the conditional access module is "releasably coupleable with the receiver." In Okabe, the only thing that appears to be releasably coupleable with anything else is the player from the terminal. Hence, the Applicant believed that the First Office Action was making this analogy (if the Examiner disagrees, than Okabe's lack of this "releasably coupleable" feature is another problem with the rejection of claim 1).

In any case, the Applicants believe that the Examiner had analogized the "player" of the Okabe reference to a "conditional access module" and the "receiver" as the terminal. Now, in rejecting claim 4, the Office Action argued that it would have been obvious that that "player" be a smartcard. In other words, that a smartcard be modified with all that is required to play a music program. In support of this proposition, the Office Action suggests that the motivation to do so would be to provide a more flexible means for distribute data. The Applicants respectfully disagreed, because a smartcard is a small secure memory device who's primary utility lies in it being credit card sized, inexpensive, and operable without batteries. A smartcard cannot be used to play music without substantial modifications which are counter to the use for which smartcards are ordinarily put. Accordingly, the Applicant cannot agree that it is obvious to modify Okabe by making substituting a smartcard for the player.

The Second Office Action now answers:

> The Examiner is confused by Applicant's interpretation and disagrees with this argument. Claim 4 indicates "wherein the conditional access module is implemented on a smartcard". The player in Okabe obviously incorporates a terminal, the use of smartcards with terminals

to assist with rights management is well known in the art. In addition, Akins teaches the use of 'smartcards' with the cable television system, in which digital data is distributed.

However, the player of Okabe does not incorporate a terminal. The player is plugged into the terminal to download and store the media.

With Respect to Claim 5: Claim 5 recites:

The method of claim 1, wherein the access control information further comprises metadata describing at least one right for the program material.

The First Office Action suggested that the foregoing discloses that the access control information includes metadata describing at least one right for the program material:

> instance **105**. Control word **117** is produced by control word generator **119** from information contained in entitlement control message **107** and information from authorization information **121** stored in set-top box **113**. For example, authorization information **121** may include a key for the service and an indication of what programs in the service the subscriber is entitled to watch. If the authorization information **121** indicates that the subscriber is entitled to watch the program of encrypted instance **105**, control word generator **119** uses the key together with information from ECM **107** to generate control word **117**. Of course, a new control word is generated for each new ECM **107**.

In fact, the foregoing discloses the opposite. It discloses that access control information is stored in the set top box, not in metadata transmitted with the access control information.

The Second Office Action responds:

> The Examiner disagrees with the argument for multiple reasons, notes that both references as a whole should be interpreted for the rejection of the claims, and again is confused by Applicant's interpretation. The passage indicates the Control word is produced from information in the entitlement control message. The Examiner interprets this to be equivalent to the control information.

The Applicant still does not understand how this discloses access control information having metadata describing at least one right for the program material.

With Respect to Claim 10: Claim 10 recites the steps of retrieving the stored re-encrypted program material and the fourth encryption key, decrypting the fourth encryption key using the third

encryption key to produce the second encryption key; and decrypting the re-encrypted material using the second encryption key. The Applicants respectfully disagree that Okabe can be modified as suggested by the Office Action.

The Office Action analogized the storage step of claim 1 to Okabe's storage of the program data in the second player. Nowhere does Okabe even remotely suggest that that data will be then retrieved by the first player from the second player. In fact, it strongly teaches away from this result. Accordingly, the Applicants cannot agree that there is any suggestion to modify as suggested.

The Second Office Action responds:

> The Examiner disagrees with this argument for multiple reasons and notes again that both references should be looked at in combination. Okabe teaches re-encrypting the program material with subsequent keys. Akins teaches retrieving program material using previously utilized keys (See passages col. 7, lines 33-38 of Okabe and col. 6 lines 24-53 of Akins).

However, Okabe does not disclose what the Second Office Action suggests, and the Examiner has not pointed to a portion of Okabe to show where this is disclosed).

With Respect to Claims 12, 13, 38, and 39: These claims recite details regarding the purchase of stored programs for replay. The Office Action suggests that these features are disclosed as follows:

> instance **105**. Control word **117** is produced by control word generator **119** from information contained in entitlement control message **107** and information from authorization information **121** stored in set-top box **113**. For example, authorization information **121** may include a key for the service and an indication of what programs in the service the subscriber is entitled to watch. If the authorization information **121** indicates that the subscriber is entitled to watch the program of encrypted instance **105**, control word generator **119** uses the key together with information from ECM **107** to generate control word **117**. Of course, a new control word is generated for each new ECM **107**.

but the Applicants disagree. Further, Okabe discloses a paradigm wherein the program material is paid for and the right to replay it determined *before* the program material is downloaded. The Applicants believe that this paradigm is antithetical to that of Akins, and hence, there is no motivation to combine the references as suggested.

"A reference may be said to teach away when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken by the applicant. The degree of teaching away will of course depend on the particular facts; in general, a reference's disclosure will teach away if it suggests that the line of development flowing from the reference's disclosure is unlikely to be productive of the result sought by the Applicant. *In re Gurley*, 27 F.3d 551, 553, 31 U.S.P.Q.2d 1130 (Fed. Cir. 1994).

VI. Dependent Claims

Dependent claims 4-16, 18-27 and 31-50 incorporate the limitations of their related independent claims, and are therefore patentable on this basis. In addition, these claims recite novel elements even more remote from the cited references. Accordingly, the Applicants respectfully request that these claims be allowed as well.

VII. New Claim

The Application has been amended to add new claim 51, which recites that the re-encrypted program material and the fourth encryption key is provided for storage external to the conditional access module.

VIII. Conclusion

In view of the above, it is submitted that this application is now in good order for allowance and such allowance is respectfully solicited. Should the Examiner believe minor matters still remain that can be resolved in a telephone interview, the Examiner is urged to call Applicants' undersigned attorney.

Respectfully submitted,

Date: April 23, 2007

By
Name: Georgann S. Grunebach
Reg. No.: 33,179

The DIRECTV Group, Inc.
CA / LA1 / A109
2230 E. Imperial Highway
P. O. Box 956
El Segundo CA 90245-0956

Telephone No. (310) 964-4615